Reducing Risk Through Managed Hosting

a guide for financial services firms

Executive Summary

As agility becomes ever more critical for business performance, managed hosting offers a highly effective way to cut costs, improve competitiveness and better exploit market opportunities. This enables firms to achieve more with fewer resources.

Given the potential competitive advantage that is at stake, even the inherently cautious financial services sector is overcoming its reticence to join the crowd in migrating to managed hosting.

However, the emerging digital risks that come with the increased speed, variety and volume of data involved, mean that in selecting the most appropriate managed hosting partner, financial services firms must take care; otherwise they risk finding their business and brand irrevocably damaged. The first step is to understand four specific risk areas: security, compliance, reputation and performance.

Overview

The recent financial crisis changed the nature of the financial services sector. Not only has it imposed new demands from consumers and regulators, but it has diminished resources and shrunk margins. As a result, more and more companies looking to reduce their IT spend, both on hardware and expertise, have turned to outsourced managed hosting.

By moving IT from a capital to an operating expense in this way, the cost savings can be considerable. The Commonwealth Bank of Australia, for example, reportedly reduced expenditure on maintenance and infrastructure from 75% of total outgoings to just 25%, as reported by Business Cloud News (2014).

Using a managed hosting service has other advantages too. These include not only enabling financial services firms to respond faster to new opportunities thanks to their enhanced and easily scalable IT capabilities, but also releasing in-house staff to focus on more strategic tasks. Tasks such as improving systems and applications, that help grow the business.

Other significant benefits of using hosted data centres include improved cyber security, reduction of physical risk such as fire and flood, seamless back-up and faster recovery.

Given these drivers, the financial services sector, along with other professional services, is increasingly recognising that maintaining and managing data securely isn't dependent on physical on-site storage. The result has been a surge in the use of managed hosting services, with Rackspace (2015) reporting that annual expenditure is set to exceed $55 billion in 2018, nearly double the $28 billion of 2014. This is in stark contrast with infrastructure-only spending, which is expected to grow at just 15 percent over the same period.

With such a growth in demand, PR Newswire (2015) has reported the number of managed hosting service providers entering the market place has already grown significantly, with a forecast compound annual growth rate (CARG) of 16.2% in provider numbers over the next five years.

However, not all these newcomers will have the functional capabilities or the necessary skills to consistently provide the services they claim to offer, or the financial robustness to survive long-term.

The Risks of Ineffective Managed Hosting

In making the move to managed hosting services, financial services companies need to be aware of four specific risk areas when selecting a suitable provider. Failure to take these into account can have potentially catastrophic consequences.

1. Security Risk

Security of data and services is now one of the greatest priorities for any financial services firm. A rapidly changing security landscape can render organisations without specialist knowledge vulnerable to breaches from random attacks, but also from an ever-growing number of concerted, coordinated and relentless campaigns, carried out with malicious or criminal intent.

As reported by State of the Internet (2015), DDoS attacks were more than double those recorded in Q2 the previous year, while further research conducted by Arbor Networks (2015) highlighted the fact that DDoS attack techniques are continuing to evolve. 126,000 SSDP-based (Simple Service Discovery Protocol) attacks were reported in the first quarter of 2015 compared with just three in the same period a year earlier.

The growing incidence of cyber attacks and data breaches brings into stark relief the monumental importance for financial service companies to protect themselves against security breaches.

Repelling such attacks has now become an ongoing cost that has to be managed on a constant basis, because when they succeed, these attacks come at such a high financial cost that many companies are unable to survive them. According to the US National Cyber Security Alliance, 60% of small businesses cease trading within six months of a successful cyber crime attack.

It is not just the loss of revenue that can be crippling – the cost of downtime is generally much greater. According to an IDC survey of IT personnel in Fortune 1000 companies, the average cost of infrastructure failure has been put at $100,000 per hour, and critical application failure at $500,000 to $1 million per hour, as reported by AppDynamics (2015).

Given the variance in duration and core costs of any one incident, calculating an accurate average total price tag for security breaches is difficult. However, research by the UK government and consultancy PwC (2015) has found that the worst data breach incidents are costing large UK businesses between £1.5m to £3m through lost sales and assets, time spent responding to the incident, and regulatory fines. For small organisations, costs were found to range from £75,200 to £310,800.

Within these figures, business disruption is the biggest component of all, costing large organisations between £800k and £2.1m (a near tripling in cost in just the space of a year), and small organisations in the realm of £40,000 to £225,000, with disruption lasting from 4 to 11 days.

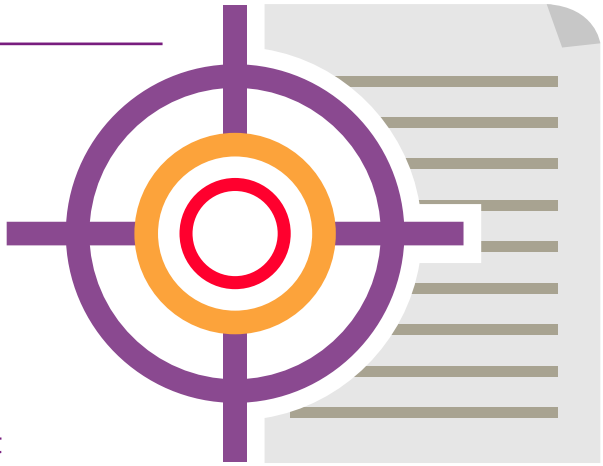
While smaller businesses have traditionally been the target for attack, larger businesses are increasingly coming under fire. Of the respondents to the survey, 90% of large organisations and 74% of small organisations suffered this type of attack in 2015, according to research by PwC (2015).

In response to emerging cyber security and fraud risk, nearly 90% of financial services firms are planning to increase their risk-management capabilities over the next two years; this comes from global management consultancy Accenture (2015) in their 2015 Global Risk Management Study.

So, whether you are an e-commerce provider processing millions of financial transactions a week, or a professional services firm storing personal information, it's crucial that any managed hosting company you select has the capacity to properly protect your data.

This means they must have not only staff who are properly security checked, but also stringent access controls, with each and every process password-protected, logged and auditable. International security accreditation ISO 27001 helps to identify hosting companies that use world-class security systems to safeguard client data. As this is fast becoming the standard required by many financial services firms and leading retailers, there could soon be a question mark over hosting providers who do not comply.

2. Compliance Risk



Being able to respond effectively and competitively to emerging regulatory standards and FSA directives has become inherently more complex in the post-financial crisis environment.

The financial services sector is facing growing and unprecedented regulatory challenges; among these challenges are ever greater supervision and stringent enforcement that is increasingly confrontational and intrusive, and to which it is not always responding well.

British financial institutions were investigated 585 times in the twelve months to April 2015 over data privacy issues, nearly three times the number recorded the previous year, according to data encryption provider, Egress Software Technology as reported in the Financial Times (2015).

While many of these incidents are attributable to issues such as inaccurate recording of data, it highlights how firms in the sector are increasingly being placed under the microscope.

So now, as well as managing 'traditional' reputation and regulatory risks such as financial crime, bribery and corruption avoidance, sanctions compliance and data protection breaches, there is an increased requirement to respond to regulatory interventions. Interventions such as ARROW visits and FSMA s166 investigations, together with emerging international standards such as US FATCA, Solvency 2 for insurers and Basel 3 for banks.

How firms manage this will be crucial to their future success. IT teams need to ensure that they have covered all the bases when it comes to being – and staying – audit ready. Selecting the right managed hosting experts can help significantly with handling the potentially overwhelming impact of current and changing regulatory requirements.

And one of the key questions for any firm in the financial services sector looking to appoint a managed hosting provider has to be, "Where is my data?"

When your data is hosted externally, getting a straight answer to this question is not always easy. However it's one which your chosen managed hosting provider should be able to give with confidence and accuracy.

The rejection of US Safe Harbour legislation means that data must be handled securely within the EU, and that will affect where your hosting provider is able to store company information.

If data is held offshore, data sovereignty, as well as security, can be a concern. On the other hand, UK-held data makes UK-based companies – and their clients – feel more secure.

3. Reputational Risk

If the sheer commercial cost of putting right a security breach wasn't enough, intimately linked to security and compliance risk is the enormous damage done to brand reputation when such events occur. With trust in the financial services sector at an all-time low, firms simply cannot afford to drop the ball, given the severity of the potential repercussions to their business.

Just a single event involving data loss or theft can seriously jeopardise the 'trust equity' that has been built up over decades. Comparatively a major breach can all too easily bring down even the seemingly most robust of firms.

While it may be tempting to play down any issue that has occurred, this often just exacerbates the situation, given the instantaneous and intense media scrutiny that can be expected to accompany any data loss event. Worse still, PwC (2015) cites that in 10% of all cases, the first a company knows about a data breach is when it is reported in the media.

The ensuing bad publicity is much more than just an embarrassment. As reported by IBM (2015) in a 2015 Cost of Data Breach Study, independent research organisation Ponemon found that 31% of those they surveyed terminated their relationship with an organisation once they knew there had been a data security breach. This has an immediate consequence for revenue, with the threat of potential legal action to recover any losses continuing to hang over the business for years to come.

It's a sobering thought that less than half of all data breaches are spotted within one day of them occurring. It's even more staggering that it takes over 100 days to pick up 8% of incidents, according to the Government's information security breaches survey 2015, published in cohort with PwC (2015).

This simply highlights the importance of having a managed hosting company on your side to act as your 'eyes and ears', especially when just 27% of these security events are detected through routine security monitoring.

4. Performance Risk

When the reputation of a business depends on the speed and efficiency of its service, failure and delay aren't an option. Yet, if in-house IT teams – an expensive resource in themselves – are unable to keep on top of their job because they're dealing with the additional responsibilities of in-house data hosting, that creates the opportunity for a 'perfect storm' of malfunction or error. In addition delay in identifying or dealing with it.

And with IT operations now so global, improving performance without compromising either the security or availability of growing volumes of data is becoming a major challenge; despite the strain which is placed on backup systems, network bandwidth and storage space.

On the other hand, a managed hosting provider will have the technical expertise to monitor, spot and manage any server issues. Therefore avoiding potentially damaging consequences for the business, should issues escalate from minor to critical.

This means not only being able to handle all necessary server maintenance, but also manage specific vulnerability issues. Issues such as dealing with continual new crops of computer bugs like GHOST, which hackers are using to gain complete control of GNU/Linux servers. Knowing that your managed hosting provider has vulnerability specialists in such areas is tremendously reassuring, and takes the weight off the shoulders of your in-house IT team, which has other roles and responsibilities.

With market forces, technological advances and customer demands forcing financial services firms to become increasingly digital, recruiting staff with the necessary skills is also a growing challenge. In such an environment, looking externally to managed hosting companies that can offer the essential specialist skills is a pragmatic and cost-effective solution.

As your business has a unique set of needs, a third party managed hosting provider will offer a wider range of benefits that you could ever achieve internally, including:

- Relevant knowledge and skills,
- Faster and easier scalability, and
- Greater economies of scale.

For you, as a financial services company, whatever your size, this means improved security and responsiveness, greater flexibility and, not least, peace of mind.

The Way Ahead in Managed Hosting

More and more companies in the financial services sector are recognising the competitive advantage that managed hosting brings, and are overcoming their natural reluctance to make the switch.

However, the value of doing so can be squandered by not choosing a managed hosting company with whom they can develop a flexible partnership to help with the proactive management of risk.

In an increasingly regulated sector, which is coming under ever tighter scrutiny, the need to balance performance against risk has never been more difficult.

While choosing from a wide variety of large established players may seem the 'safe' bet, one of a new generation of managed hosting providers, with a less 'restrictive' approach, may offer a more cost-effective, yet still robust solution. Meeting both escalating data storage needs and cyber-security concerns.

One of the reasons for using a managed hosting service is to benefit from a low initial capital outlay, followed by predictable monthly costs long-term, with no unexpected charges or revisions.

With large managed service companies this isn't always the case, as their periodic usage reviews can hike up rates. Once they're embedded in your business operations, you have little option but to pay.

While it is understandably tempting to choose the lowest-cost provider in the short-term, there may be higher long-term costs.

Finding a flexible supplier with whom you can negotiate an individual service level agreement may be a better option.

Managed hosting is a bespoke service that can and should be tailored to a customer's individual needs, rather than a one size fits all solution. Potential service providers should want to work with you to create a bespoke hosting solution that meets both your unique requirements as a business, and your budget.

Then, as your managed hosting requirements change, as they almost certainly will in a highly dynamic market, that solution can be scaled up or consolidated downwards for greater cost control.

On the other hand, given that they are in a volume market, large managed hosting companies may view you as 'just another customer' to whom they must sell their largest, most comprehensive package.

The **personal service** you get with smaller providers is a reflection of the greater flexibility they are likely to provide. Having a single point of contact for instance, not only removes the need to repeat time-consuming conversations about what are often business-critical problems, but also helps ensure there is direct communication between the provider and you as the customer. Something which is invaluable in getting to know you and your business.

Rather than seeing themselves as an external supplier, the smaller provider will work with you to identify specific solutions to limit the potential damage arising from the four main risk areas described above. In other words, they will be proactive in preventing problems arising, rather than acting as fire-fighters rushing from one incident to another.

Smaller managed hosting providers are more likely to encourage a **partnership approach**, in which their success is tied to yours, and the added value they bring will make them an indispensable long-term asset. They will see any breach or data loss as a shared problem rather than the client's alone. Some larger hosting companies tend to put their interests first, leaving the client to pay the price of a damaged reputation and lost revenues, in some cases sufficient to ruin a smaller company.

Using outsourced managed hosting can help firms in the financial services sector to achieve competitive advantage by reducing their costs and improving their responsiveness. However, choosing the right provider among a range of larger established companies and often untested newcomers, can be difficult.

In this whitepaper we have described the four specific risk areas — **security, compliance, reputation and performance** — that must be given particular consideration during the selection process. This will help to avoid the risks inherent in managing the increased speed, variety and volume of data that is now at the very core of the financial services sector.

About Digital Craftsmen

As hosting experts, we provide bespoke hosting and managed services to financial services firms looking to maximise performance and profitability without compromising data security. Since setting up Digital Craftsmen back in 2002, it has been our aim to bring the human touch to a service that is often offered impersonally and entirely online. That means we will go out of our way to become in effect an extension of your own in-house team, providing a service that is flexible, personal and tailored to your exact specification.

Digital Craftsmen Limited
1 Fore Street
London
EC2Y 5EJ

0845 519 5292

www.digitalcraftsmen.com

REFERENCES

ACCENTURE (2015) "2015 Global Risk Management Study: Paths to prosperity" [online] available from https://www.accenture.com/us-en/global-risk-management-research-2015.aspx [Accessed: 5th January 2016]

APPDYNAMICS (2015) "The Real Cost of Downtime, The Real Potential of DevOps" [online] available from https://blog.appdynamics.com/devops/idc-devops-cost-downtime/ [Accessed: 5th January 2016]

ARBOR NETWORKS (2015) "Arbor Networks Detects Largest Ever DDoS Attack in Q1 2015 DDoS Report" [online] available from http://www.arbornetworks.com/news-and-events/press-releases/2015-press-releases/5405-arbor-networks-records-largest-ever-ddos-attack-in-q1-2015-ddos-report [Accessed: 5th January 2016]

BUSINESS CLOUD NEWS (2014) "Cloud in financial services – what is it not good for?" [online] available from http://www.businesscloudnews.com/2014/06/02/cloud-in-financial-services-what-is-it-not-good-for/ [Accessed: 5th January 2016]

FINANCIAL TIMES (2015) "Probes into data breaches at UK financial firms triple" [online] available from http://www.ft.com/cms/s/74314ae6-0943-11e5-b643-00144feabdc0,Authorised=false.html?siteedition=uk&_i_ location=http%3A%2F%2Fwww.ft.com%2Fcms%2Fs%2F0%2F74314ae6-0943-11e5-b643-00144feabdc0.html%3Fsiteedition%3Duk&_i_referer=&classification=conditional_standa [Accessed: 5th January 2016]

IBM (2015) "2015 Cost of Data Breach Study" [online] available from http://www-03.ibm.com/security/data-breach/ [Accessed: 5th January 2016]

PR NEWSWIRE (2015) "Global Cloud Infrastructure Market 2015-2020 - Managed Hosting Services are Expected to Grow at a CARG of 16.2% by 2020" [online] available http://www.prnewswire.com/news-releases/global-cloud-infrastructure-market-2015-2020---managed-hosting-services-are-expected-to-grow-at-a-carg-of-162-by-2020-300127430.html [Accessed: 5th January 2016]

PwC (2015) "2015 Information Security Breaches Survey: Technical Report" [online] available from http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf [Accessed: 5th January 2016]

RACKSPACE (2015) "The Growing Market for Managed Cloud" [online] available from http://blog.rackspace.com/the-growing-market-for-managed-cloud/ [Accessed: 5th January 2016]

STATE OF THE INTERNET (2015) "Q2 2015 State of the Internet – Security Report" [online] available from https://www.stateoftheinternet.com/resources-cloud-security-2015-q2-web-security-report.html [Accessed: 5th January 2016]